

# UNITED STATES DISTRICT COURT

for the  
Western District of Washington

FILED	LODGED
RECEIVED	
May 15, 2020	
CLERK U.S. DISTRICT COURT WESTERN DISTRICT OF WASHINGTON AT TACOMA	
BY	DEPUTY

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)  
The SUBJECT DEVICE DataLocker (IronKey)  
External Hard Drive MORE FULLY DESCRIBED IN  
ATTACHMENT B.

Case No. MJ20-5116

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT B, ATTACHED HERETO AND INCORPORATED HEREIN BY REFERENCE.

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

SEE ATTACHMENT C, ATTACHED HERETO AND INCORPORATED HEREIN BY REFERENCE.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 2252(a)(2)	Receipt or Distribution of Child Pornography
18 U.S.C. § 2252(a)(4)(B)	Possession of Child Pornography

The application is based on these facts:

- ☒ See Affidavit of Homeland Security Investigations Special Agent, Ly Tran.

☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means; or: ☐ telephonically recorded.

*Ly C Tran*

Applicant's signature

Ly Tran, Special Agent HSI

Printed name and title

- ☐ The foregoing affidavit was sworn to before me and signed in my presence, or
- ☒ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 5-15-2020

*David W Christel*

Judge's signature

City and state: Tacoma, Washington

DAVID W. CHRISTEL United States Magistrate Judge

Printed name and title

**AFFIDAVIT OF LY TRAN**

STATE OF WASHINGTON )  
 ) ss  
 COUNTY OF PIERCE )

I, Ly Tran, a Special Agent with the Homeland Security Investigations, Seattle, Washington, having been duly sworn, state as follows:

**I. Affiant Background**

1. I am a Special Agent with Homeland Security Investigations (HSI) currently assigned to the Border Enforcement Security Task Force in Seattle, Washington. I have been employed by HSI, formerly known as Immigration and Customs Enforcement, since May 2005. Prior to my employment with HSI, I was a Parole Officer for the State of Washington Department of Corrections for approximately four years.

2. I have completed the Criminal Investigators Training Program and Immigration and Customs Enforcement Special Agent Training at the Federal Law Enforcement Training Center in Glynco, Georgia. I have also completed the Drug Enforcement Administration Basic Drug Enforcement Training. I am familiar with investigations of drug trafficking organizations, methods of importation and exportation, distribution and smuggling of controlled substances, and financial and money laundering investigations. I have participated in numerous investigations involving organizations trafficking in controlled substances, including, ecstasy, marijuana, and cocaine which, have resulted in the arrest of drug traffickers and seizures of controlled substances and currency. I have participated in the execution of search warrants for controlled substances; and have personally been involved in the seizures of controlled substances. Additionally, I have participated in investigations involving human trafficking, financial crimes, cybercrimes, and murder for hire. While assigned to the HSI Attaché office in Vietnam, I conducted numerous investigations involving the sexual exploitation of

1 children and interstate / international travel for illegal sexual activity involving minors.  
 2 During the course of these investigations, I have reviewed child exploitation materials.

## 3 **II. Purpose Of Affidavit**

4 3. This application for issuance of a search warrant is being presented by  
 5 reliable electronic means pursuant to Federal Rule of Criminal Procedure 4.1 and Local  
 6 Criminal Rule 41(d)(3). During a lawfully authorized search of an email account,  
 7 authorized to search for evidence of a scheme to illegal import Japanese Kei cars, your  
 8 affiant came across evidence of other criminal activity: namely, images of child  
 9 pornography. Consequently, I make this affidavit in support of an application for a  
 10 search warrant authorizing the expanded examination an electronic storage media,<sup>1</sup>  
 11 already in the possession of the United States, hereinafter the "SUBJECT DEVICE." I  
 12 further seek to extract evidence from the electronic storage media, the nature of which is  
 13 more specifically described in Attachment C. The SUBJECT DEVICE is further  
 14 described in Attachment B. The SUBJECT DEVICE is currently in law enforcement  
 15 possession as the fruit of a prior search warrant. A copy of the original application,  
 16 affidavit, and warrant is attached hereto as Attachment A.

17 4. The facts set forth in this Affidavit are based on my own personal  
 18 knowledge; knowledge obtained from other individuals during my participation in this  
 19 investigation, including other law enforcement officers; review of documents and records  
 20 related to this investigation; communications with others who have personal knowledge  
 21 of the events and circumstances described herein; and information gained through my  
 22 training and experience. Because this Affidavit is submitted for the limited purpose of  
 23 establishing probable cause in support of the application for a search warrant, it does not  
 24 set forth each and every fact that I or others have learned during the course of this

---

25  
 26  
 27 <sup>1</sup> Electronic Storage media is any physical object upon which electronically stored information can be recorded.  
 28 Examples include external hard drive, hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.



1 investigation. I have set forth only the facts I believe are relevant to the determination of  
 2 probable cause to believe evidence, fruits, and instrumentalities of violations of 18 U.S.C.  
 3 § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. §  
 4 2252(a)(4)(B) (Possession of Child Pornography), will be found in the SUBJECT  
 5 DEVICE.

### 6 **III. Summary of Vehicle Importation/Smuggling Investigation**

7 5. In October 2019, I met with the U.S. Customs and Border Protection (CBP)  
 8 officers in Seattle, Washington. According to these CBP officers, and based on my  
 9 examination of specific import documents, CHRISTOPHER COX appears to have  
 10 imported twenty vehicles into the United States using false, fraudulent, and counterfeit  
 11 documents. Specifically, the CBP Officers believed, and my analysis of documents and  
 12 interviews of witnesses confirms, that CHRISTOPHER COX falsified documents/seals  
 13 from CBP, from the Environmental Protection Agency (EPA), and from the U.S.  
 14 Department of Transportation (DOT) to smuggle the cars into the United States.  
 15 CHRISTOPHER COX also used false and fraudulent information to gain access to secure  
 16 areas of the Port of Tacoma, claiming that he was importing vehicles for the United  
 17 States Postal Service, which enabled him to evade all required CBP inspections of the  
 18 cars he illegally smuggled into the United States. CHRISTOPHER COX then used the  
 19 fraudulent, false, and counterfeit documents to register and license the vehicles, and later  
 20 sold the vehicles to unsuspecting customers. Because of CHRISTOPHER COX's  
 21 criminal activities, it appears that up to twenty buyers purchased and are now driving  
 22 extremely unsafe, illegal cars that never should have been licensed for on-road and  
 23 highway use.

### 24 **IV. Search Warrant Email Account [cctc53611@gmail.com](mailto:cctc53611@gmail.com)**

25 6. As part of my investigation of the vehicle importation/smuggling  
 26 summarized above, I applied for and obtained a search warrant for CHRISTOPHER  
 27 COX email account [cctc53611@gmail.com](mailto:cctc53611@gmail.com) (MJ20-5061—Attachment A). The search  
 28



1 warrant required Google Inc. to disclose to the government copies of the contents of all  
2 emails (including the content of communications) associated with the account, including  
3 stored or preserved copies of emails sent to and from the account, draft emails, the source  
4 and destination addresses associated with each email, the date and time at which each  
5 email was sent, and the size and length of each email, and any attachments to such  
6 emails.

7 7. On March 23, 2020, I served the search warrant in Attachment A for the  
8 email account via Google's law enforcement services portal: [lers@google.com](mailto:lers@google.com). On April  
9 13, 2020, Google responded to the search warrant and provided me a download link for  
10 approximately eighty-three (83) zipped files contained data, pictures, video clips, and  
11 documents. Google Inc. advised me that the download link would expire in fourteen (14)  
12 days; therefore, I downloaded the data to the SUBJECT DEVICE for further reviewing  
13 and analyzing. The SUBJECT DEVICE is a passcode secure device manufactured by  
14 Datalocker.

15 8. The focus of the original search warrant (Attachment A) was to find  
16 evidence of the scheme to illegally import Kei cars and trucks. I began reviewing the  
17 files for this evidence on April 17, 2020. The files were typically identified or labeled as  
18 follows, 3610661-20200413-1, 3610661-20200413-2, 3610661-20200413-3... to  
19 3610661-20200413-42, and 3610661-20200414-1, 3610661-20200414-2, 3610661-  
20 20200414-3...to 3610661-20200414-41. Each of these files had many subfiles and  
21 subfolders.

22 9. On April 22, 2020, I reviewed data/materials in folder number 3610661-  
23 20200413-10 -> cctc53611.846325528617.GooglePhotos.PhotoResource\_038.Preserved  
24 -> Google Photos -> Wow. In the subfolder titled "Wow," I observed numerous  
25 pornographic pictures and video clips. When I clicked on file name "images (13)," I  
26 observed what appeared to be a naked underage white female showing her genital area. I  
27 then clicked on another file name "younowjoe\_jbs\_younow\_youtube\_cam0545.avi." I  
28

1 observed one picture containing numerous smaller pictures of what appeared to be naked  
2 underage white females. I stopped the search and contacted Assistant United States  
3 Attorney David Reese Jennings and HSI Special Agent Cao Triet (Dan) Huynh. Special  
4 Agent Huynh is currently assigned to the HSI Seattle Human Exploitation and Cyber  
5 Crimes Group. Special Agent Huynh is also a member of the Seattle Internet Crimes  
6 Against Children Task Force. Special Agent Huynh has ten years experience conducting  
7 child exploitation investigations. I stopped my review of the files obtained with the  
8 original search warrant to determine my next steps.

9 10. On April 23, 2020, I met with Special Agent Huynh. I guided Special  
10 Agent Huynh to the two files that appeared to contain images of child exploitation. Upon  
11 reviewing the images, Special Agent Huynh and I concluded the pictures were child  
12 exploitation materials. The pictures are further described as follow by Special Agent  
13 Huynh and I:

14 **File images (13):**

15 11. Image (13) is a color image. It depicts what appears to be a white  
16 prepubescent female (hereinafter referred to as child victim) positioned and posed sitting  
17 on what appears to be pink carpet. The child victim is not wearing any clothes, and she  
18 has long blond hair. Her back is against a wall with base molding. The child victim is  
19 leaning/resting her face on her hands and looks at the camera. The child victim has her  
20 elbows resting on her thighs, and her legs spread across the width of the image, towards  
21 the camera exposing her vaginal area. The child victim does not have pubic/body hair.  
22 The child victim is small and does not have developed breasts. The child victim's face is  
23 youthful in appearance, and she appears to be under the age of 10.

24 **File younowjoe\_jbs\_younow\_youtube\_cam0545.avi:**

25 12. File younowjoe\_jbs\_younow\_youtube\_cam0545.avi is a vid-cap (still  
26 image consisting of a frame captured from film or television) photo. It has fourteen (14)  
27 smaller pictures of a white prepubescent female (hereinafter referred to as child victim)  
28



1 positioned and posed in front of camera. The child victim is wearing a black tan top. She  
2 has long blond hair. The child victim is sitting next to what appears to be white pillow  
3 with red stripes. The first two pictures appeared to be the child victim waving and  
4 smiling to the camera. The vid-cap image then progressively shows the child victim's  
5 genital/anus area and inserting her finger into her genital area. The child victim does not  
6 have pubic/body hair. The child victim is small and does not have developed breasts.  
7 The child victim's face is youthful in appearance, and she appears to be under the age of  
8 12.

9 **V. Information To Be Searched And Items To Be Seized**

10 13. If a new search warrant is issued in response to this application, I and/or  
11 other law enforcement personnel will continue reviewing the contents of the  
12 electronically stored data and identify from among that content those items that come  
13 within the items identified in Section II to the applicable Attachment C, for seizure. I  
14 will also continue my search pursuant to the original warrant (Attachment A).

15 14. Analyzing the data contained in the forensic image may require special  
16 technical skills, equipment, and software. It could also be very time-consuming.  
17 Searching by keywords, for example, can yield thousands of "hits," each of which must  
18 then be reviewed in context by the examiner to determine whether the data is within the  
19 scope of the warrant. Merely finding a relevant "hit" does not end the review process.  
20 Keywords used originally need to be modified continuously, based on interim results.  
21 Certain file formats, moreover, do not lend themselves to keyword searches, as keywords,  
22 search text, and many common email, database and spreadsheet applications do not store  
23 data as searchable text. The data may be saved, instead, in proprietary non-text format.  
24 In addition, as the volume of storage allotted by service providers increases, the time it  
25 takes to properly analyze recovered data increases, as well. Consistent with the  
26 foregoing, searching the recovered data for the information subject to seizure pursuant to  
27 this warrant may require a range of data analysis techniques and may take weeks or even  
28



1 months. All forensic analysis of the data will employ only those search protocols and  
2 methodologies reasonably designed to identify and seize the items identified in Section II  
3 of Attachment C to the warrant.

4 15. Based on my experience and training, and the experience and training of  
5 other agents with whom I have communicated, it is necessary to review and seize a  
6 variety of messenger communications, chat logs, files, payment records and documents,  
7 that identify any users of the subject account and communications sent or received in  
8 temporal proximity to incriminating messages that provide context to the incriminating  
9 communications.

#### 10 VI. Sealing Request

11 16. It is respectfully requested that the Court issue an order sealing, until  
12 further order of the Court, all papers submitted in support of the requested warrants,  
13 including the application, this affidavit, the attachments, and the requested warrants. I  
14 believe that sealing these documents is necessary because the information to be seized is  
15 relevant to an ongoing investigation and includes references to cooperating individuals.  
16 Premature disclosure of the contents of the application, this affidavit, the attachments,  
17 and the requested warrants may adversely affect the integrity of the investigation,  
18 including giving targets a chance to destroy evidence or take other steps to hinder the  
19 investigation.

#### 20 VII. Conclusion

21 17. Based upon the evidence gathered in this investigation as set out above,  
22 including but not limited to my review of data and records, information received from  
23 other law enforcement agents, and my training and experience, there is probable cause to  
24 believe evidence, fruits and/or instrumentalities of the crimes of 18 U.S.C. §§ 2252(a)(2)  
25 (Receipt or Distribution of Child Pornography) and 2252(a)(4)(B) (Possession of Child  
26 Pornography) exists and will be found in the SUBJECT DEVICE, and any attachments,  
27 stored instant messages, stored voice messages, documents, and photographs associated  
28

1 therewith, as well as in subscriber and log records associated with the account.  
2 Accordingly, by this Affidavit and warrant I seek authority for the government to search  
3 all of the items specified in Attachment B and Section I of Attachment C (attached hereto  
4 and incorporated by reference herein) to the warrant, and specifically to seize all of the  
5 data, documents and records which are identified Section II of Attachment C.

6 18. The United States requests that the Court order that this application and any  
7 resulting order be sealed until further order of the Court. As explained above, these  
8 documents discuss an ongoing criminal investigation that is neither public nor known to  
9 all of the targets of the investigation. Accordingly, there is good cause to seal these  
10 documents because their premature disclosure may seriously jeopardize that  
11 investigation.

12 *Ly C Tran*

13 LY TRAN

14 Special Agent

Homeland Security Investigations

15 The above-named agent provided a sworn statement attesting to the truth of the  
16 contents of the foregoing affidavit on this 15<sup>th</sup> day of May, 2020.

17 *DW Christel*

18 DAVID W. CHRISTEL

19 United States Magistrate Judge  
20  
21  
22  
23  
24  
25  
26  
27  
28

# ATTACHMENT A



## UNITED STATES DISTRICT COURT

for the  
Western District of Washington

FILED	LODGED
RECEIVED	
MAR 17 2020	
CLERK U.S. DISTRICT COURT WESTERN DISTRICT OF WASHINGTON AT TACOMA	
BY	DEPUTY

## In the Matter of the Search of

(Briefly describe the property to be searched  
or identify the person by name and address)INFORMATION ASSOCIATED WITH GOOGLE  
ACCOUNT cctc53611@gmail.com MORE FULLY  
DESCRIBED IN ATTACHMENT A.

Case No.

MJ20-5061

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A, ATTACHED HERETO AND INCORPORATED HEREIN BY REFERENCE.

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

SEE ATTACHMENT B-1, ATTACHED HERETO AND INCORPORATED HEREIN BY REFERENCE.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

## Code Section

18 USC §§ 506, 545, 1001,  
1036, and 1343

## Offense Description

Fraudulently using Seals of Department or Agencies, Smuggling Goods into the United States, Falsely Impersonating an Officer or Employee of the United States, Making Material False Statements, Making Entry to a Secure Area of a Seaport by False Pretenses and Committing Fraud by wire, radio, or television.

The application is based on these facts:

- ☒ See Affidavit of Homeland Security Investigations Special Agent, Ly Tran.

☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means; or: ☐ telephonically recorded.

Applicant's signature

Ly Tran, Special Agent HSI

Printed name and title

- ☐ The foregoing affidavit was sworn to before me and signed in my presence, or
- ☒ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 3-17-2020

Judge's signature

City and state: Tacoma, Washington

Theresa L. Fricke, United States Magistrate Judge

Printed name and title

**ATTACHMENT A**

**SUBJECT ACCOUNT to be Searched**

The electronically stored data, information and communications contained in, related to, and associated with, including all preserved data associated with the Google account cctc53611@gmail.com, as well as all other subscriber and log records associated with the account, which is stored at premises owned, maintained, controlled, or operated by Google Inc., an electronic communications services and remote computing services provider located at 1600 Amphitheatre Parkway, Mountain View, California 94043.

**ATTACHMENT B****Section I - Information to be disclosed by Google for search:**

To the extent that the information described in Attachment A-1 is within the possession, custody, or control of Google, including any emails, records, files, logs, or information that has been deleted but is still available to Google. Google is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email, and any attachments to such emails;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, instant messages, and instant messenger contact information, calendar data, pictures, and files.

e. All records pertaining to communications between Google and any person regarding the account, including contacts with support services and records of actions taken.



**Section II - Information to be seized by the government**

All information described above in Section I that constitutes contraband, evidence, fruits, or instrumentalities of the following crimes committed on or after November 30, 2017: Title 18, United States Code, Section 506 – Seals of Department or Agencies, Title 18 United States Code, Section 545 – Smuggling Goods into the United States, Title 18 United States Code, Section 912 – Officer or Employee of the United States, Title 18 United States Code, Section 1001 False Statements, Title 18 United States Code Section 1036, Entry by False Pretenses to an real Property, Vessel, or Aircraft of the United States or Secure Area of any Airport or Seaport, and Title 18 United States Code, Section 1343 - Fraud by wire, radio, or television.

a. All messages, documents, and profile information, attachments, or other data that serves to identify any persons who use or access the account specified, or who exercise in any way any dominion or control over the specified account

b. Any address lists or “friend”/contact lists associated with the specified account;

c. All subscriber records associated with the specified account, including name, address, local and long distance telephone connection records, or records of session times and durations, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address, and means and source of payment for such service) including any credit card or bank account number;

d. Any and all other log records, including IP address captures, associated with the specified account;

e. Any records, documents, forms, attachments, photographs, and pictures relating to importation of vehicles and vehicle parts;

f. Any records and email communications to and from Be Forward Co. Ltd., and Sound Brokerage; and

1 g. Any records of communications between Google and any person about issues  
2 relating to the account, such as technical problems, billing inquiries, or complaints from  
3 other users about the specified account. This to include records of contacts between the  
4 subscriber and the provider's support services, as well as records of any actions taken by  
5 the provider or subscriber as a result of the communications.

6 Google is hereby ordered to disclose the above information to the government  
7 within 14 days of service of this warrant.  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**I. AFFIDAVIT OF LY TRAN**

STATE OF WASHINGTON )  
 ) ss  
 COUNTY OF PIERCE )

I, Ly Tran, a Special Agent with the Homeland Security Investigations, Seattle, Washington, having been duly sworn, state as follows:

**II. Affiant Background**

1. I am a Special Agent with Homeland Security Investigations (HSI) currently assigned to the Border Enforcement Security Task Force in Seattle, Washington. I have been employed by HSI, formerly known as Immigration and Customs Enforcement, since May 2005. Prior to my employment with HSI, I was a Parole Officer for the State of Washington Department of Corrections for approximately four years.

2. I have completed the Criminal Investigators Training Program and Immigration and Customs Enforcement Special Agent Training at the Federal Law Enforcement Training Center in Glynco, Georgia. I have also completed the Drug Enforcement Administration Basic Drug Enforcement Training. I am familiar with investigations of drug trafficking organizations, methods of importation and exportation, distribution and smuggling of controlled substances, and financial and money laundering investigations. I have participated in numerous investigations involving organizations trafficking in controlled substances, including, ecstasy, marijuana, and cocaine which, have resulted in the arrest of drug traffickers and seizures of controlled substances and currency. I have participated in the execution of search warrants for controlled substances; and have personally been involved in the seizures of controlled substances. Additionally, I have participated in investigations involving human trafficking, financial crimes, murder for hire, traveling child sex investigations, and cybercrimes.



### III. Purpose Of Affidavit

3. This application for issuance of a search warrant is being presented by reliable electronic means pursuant to Federal Rule Criminal Rule Procedure 4.1 and Local Criminal Rule 41(d)(3). Specifically, this Affidavit is submitted in support of an application for a search warrant for information associated with a certain account that is stored at premises controlled Google, and e-mail provider headquartered at Mountainview, California. The information to be searched is connected to the Gmail account "cctc53611@gmail.com," associated with CHRISTOPHER COX, date of birth August 20, 1972, as further described in this affidavit and detailed in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

4. The facts set forth in this Affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; review of documents and records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience. Because this Affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation.

5. As set forth below, there is probable cause to believe that the Gmail account will contain evidence of how Christopher Cox repeatedly smuggled tiny Japanese "Kei" cars into the United States, using counterfeit images of federal seals, by

1 violating federal smuggling laws, by falsely impersonating an officer or employee of the  
2 United States, by making materially false entries in federal records, by using false  
3 pretenses to enter a secure area in Seaport, and by committing fraud by wire. These acts  
4 amount to violations of Title 18, United States Code, Sections 506 (Fraudulently using  
5 Seals of Department or Agencies) 545 (Smuggling Goods into the United States), 912  
6 (Falsely Impersonating an Officer or Employee of the United States) 1001 (Making  
7 Material False Statements) 1036 (Making Entry to a Secure Area of a Seaport by False  
8 Pretenses) and 1343 (Committing Fraud by wire, radio, or television). I seek  
9 authorization to search and seize the items specified in Attachment B, which is  
10 incorporated herein by reference.

#### 11 **IV. Summary Of Investigation**

12 6. In October 2019, I met with the U.S. Customs and Border Protection (CBP)  
13 officers in Seattle, Washington. According to these CBP officers, and based on my  
14 examination of specific import documents, CHRISTOPHER COX appears to have  
15 imported twenty vehicles into the United States using false, fraudulent, and counterfeit  
16 documents. Specifically, the CBP Officers believed, and my analysis of documents and  
17 interviews of witnesses confirms, that COX falsified documents/seals from CBP, from  
18 the Environmental Protection Agency (EPA), and from the U.S. Department of  
19 Transportation (DOT) to smuggle the cars into the United States. CHRISTOPHER COX  
20 also used false and fraudulent information to gain access to secure areas of the Port of  
21 Tacoma, claiming that he was importing vehicles for the United States Postal Service,  
22 which enabled him to evade all required CBP inspections of the cars he illegally  
23 smuggled into the United States. COX then used the fraudulent, false, and counterfeit  
24 documents to register and license the vehicles, and later sold the vehicles to unsuspecting  
25 customers. Because of COX's criminal activities, it appears that up to twenty buyers  
26 purchased and are now driving extremely unsafe, illegal cars that never should have been  
27 licensed for on-road and highway use.  
28

V. **What is a Kei Vehicle?**

7. Kei car (or keijidōsha "light automobile," pronounced [ke:dzido:ɕa]) is the Japanese vehicle category for the smallest highway-legal passenger cars available in Japan. Similar Japanese categories exist for microvans, and Kei trucks. The Kei car category was created by the Japanese government in 1949, and the regulations have been revised several times since. Japanese regulations specify a maximum vehicle size, engine capacity of 660cc and power output. Owners of Kei cars and vehicles in Japan enjoy both tax and insurance benefits.

8. Kei cars have become very successful in Japan — consisting of over one third of domestic new car sales in fiscal 2016. In 2018, seven of the 10 top-selling car models in Japan were Kei cars, including the top four—all of which were boxy passenger vans. In export markets such as the United States, Kei cars are generally too specialized and too small. In fact, most Kei-cars are not exportable outside of Japan, for the good and only reason that they do not comply with most American and European crash standards.

9. The Imported Vehicle Safety Compliance Act, commonly known as the 25-year import rule, prevents individuals from importing new foreign-market vehicles without undertaking a lengthy testing and federalization process. The law is intended to keep American drivers safe. Any car brought into the United States that is less than 25 years old must meet all U.S. safety and crashworthiness standards (unless brought in for off-road use only). The assumption behind this law is that fewer and fewer of any unsafe and noncompliant car will be available for import after 25 years, thus decreasing the risk that they will be imported to the United States for practical use. When the law was passed, those who drafted it considered cars older than 25 years to be “classics” or “antiques.” The 25-year rule represented a compromise: collectors could still have their cars, but the average American was going to need to buy something the government and manufacturers could assure was safe and fit for American roads. The law protected



1 drivers (from injury and accident), automobile manufacturers (from liability), but allowed  
2 collectors eventual access to desired cars.

3 10. In addition to the 25-year rule for vehicle safety, the Environmental  
4 Protection Agency also has laws that cover imported cars. Basically, cars less than 21  
5 years old must actually meet federal emissions standards. Cars older than 21 years may  
6 be exempted from federal emissions standards.

7  
8 **VI. Background and Importation Procedure of a Vehicle:**

9 11. Importers must file multiple certifications and declarations with CBP when  
10 they attempt to import a vehicle into the United States. The purpose of the certifications  
11 is to ensure that the imported vehicle complies with the United States transportation,  
12 safety, and environmental regulations. The EPA mandates that an importer file a  
13 declaration with CBP indicating that a vehicle conforms to the environmental standards  
14 required of U.S. vehicles. The DOT mandates that an importer file a declaration with  
15 CBP indicating that a vehicle conforms to national safety standards.

16 12. All those who attempt to import a vehicle must submit the following  
17 documents at the time of entry:

- 18 a. Bill of Lading
- 19 b. Bill of Sale
- 20 c. Registration from country of origin (export certificate)
- 21 d. Proof of ownership
- 22 e. EPA Form 3520-1 showing emissions compliance / exemption
- 23 f. DOT HS-7 showing safety compliance / exemption
- 24 g. Manufacturers label on engine showing emissions requirements (in
- 25 English)
- 26
- 27
- 28

1        13. Importers must also attest to whether the imported vehicle is over 25 years  
 2 old. If a vehicle is over 25 years old, CBP is required to verify the Vehicle Identification  
 3 Number (VIN) to determine the age of the vehicle and to review the following  
 4 documents:

- 5            a. EPA and DOT paperwork
- 6            b. Export certificate
- 7            c. Ownership documentation
- 8            d. Invoice
- 9            e. CBP Form 7501 (Entry Documentation)

10  
 11        14. If a vehicle is less than 25 years old, the importer must have and present a  
 12 certified letter from the vehicle's manufacturer, indicating that the vehicle conforms to  
 13 EPA / DOT regulations. The letter must be issued by the U.S.-based arm of the vehicle's  
 14 manufacturer.

15        15. Once an importer files all required entry documents on a vehicle to be  
 16 imported into the United States through the Port of Tacoma, Washington, he or she is  
 17 then required to pick up the vehicle from the East Blair 1 Terminal, 2940 East Alexander  
 18 Avenue, Tacoma, WA. The importer must then present the vehicle for inspection to CBP  
 19 Officers at 2202 Port of Tacoma Road, Tacoma, WA (within the Port of Tacoma). Once  
 20 CBP inspects the vehicle, CBP will either approve or disapprove the entry documents. If  
 21 CPB approves the entry documents, CBP Officers will stamp the import/entry documents  
 22 with the Department of Homeland Security's seal. The importer may then present the  
 23 approved entry documents to the Washington State Department of Licensing.

24                    **VII. Vehicles Imported by CHRISTOPHER COX**

25        16. On October 17, 2019, I received import/entry summary packages for  
 26 vehicles identified as having been imported by CHRISTOPHER COX through the Port of  
 27 Tacoma. These vehicles were identified by importation documents from CBP and  
 28

1 vehicle registration documents from Washington State Department of Licensing. They  
2 include the following:

- 3 1. Used 2007 Honda Odyssey, VIN # RB13313672, Entry date February 15,  
4 2018, Entry # BMG0518081-8, Reference # BF717260.
- 5 2. Used 2013 Toyota Probox Van, VIN # DBENC50V (or NCP 51  
6 0303096), Entry date February 15, 2018, Entry # BMG-0518087-5
- 7 3. Used 2007 Nissan Otti, VIN # H92WW0001474, Entry date April 12,  
8 2018, Entry # BMG 0518236-8, Reference # BF767867
- 9 4. Used 2002 Honda Life, VIN # JB16206491, Entry date April 19, 2018,  
10 Entry # BMG-0518335-8, Reference # BF770103
- 11 5. Used 2013 Nissan AD Van, VIN # VAY12 069032, Entry date June 11,  
12 2018, Entry # BMG-0518611-2, Reference # BF794517
- 13 6. Used 2006 Honda Mobilio, VIN # GB1-1702091, Entry date September  
14 14, 2018, Entry # BMG-0519101-3, Reference # BF863236
- 15 7. Used 2001 Subaru Legacy Touring Wagon, VIN # BH5120390, Entry date  
16 October 26, 2018, Entry # BMG-0519391-0 Reference # BG004916
- 17 8. Used 2001 Subaru Legacy Touring Wagon, VIN # BH5182300, Entry date  
18 November 08, 2018, Entry # BMG-0519463-7, Reference # BF954503
- 19 9. Used 2013 Nissan AD Van, VIN # VZNY12-039945, Entry date  
20 November 14, 2018, Entry # BMG-0519455-3, Reference # BF952646
- 21 10. Used 2005 Subaru Legacy Touring Wagon, VIN # BP5099663, Entry date  
22 December 30, 2018. Entry # BMG-0519630-1, Reference # BG038672
- 23 11. Used 2008 Daihatsu Move Latte, VIN # L560S0022409, Entry date  
24 December 31, 2018, Entry # BMG-0519631-9, Reference # BG050263
- 25 12. Used 2001 Honda Vamos, HM21204538, Entry date January 11, 2019,  
26 Entry # BMG-0519661-6, Reference # BG058910
- 27 13. Used 2003 Subaru Legacy Touring Wagon, VIN # BP5033963, Entry date  
28 May 8, 2019, Entry # BMG-0520179-6, Reference # BG158395



1 14. Used 2005 Subaru Legacy Touring Wagon, VIN # BP5049938, Entry date  
2 May 08, 2019, Entry # BMG-0520178-8, Reference # BG141625

3 15. Used 2009 Mitsubishi Minicab Truck, VIN # U61T 1401320, Entry date  
4 June 3, 2019, Entry # BMG-0520143-2, Reference # BG186391

5 16. Used 2006 BMW 3 Series, VIN # WBABX92030PN92388, Entry date  
6 June 21, 2019, Entry # BMG-0520562-3, Reference # BG193744

7 17. Used 2004 Subaru Legacy Touring Wagon, VIN # BP5035373, Entry date  
8 July 07, 2019, Entry # BMG-0520470-9, Reference # 07/07/2019

9 18. Used 2012 Mitsubishi Lancer Cargo, VIN # VZNY12610535, Entry date  
10 July 7, 2019, Entry # BMG-0520471-9, Reference # BG206654

11 19. Used 2000 Daihatsu Atrai Wagon, VIN # S220G00016550, Entry date  
12 September 09, 2019, Entry # BMG-0520816-3 (detained by CBP in Tacoma)

13 20. Used 2007 Mazda Bongo Van, VIN # SK82V-322838, Entry date  
14 September 9, 2019, Entry # BMG-0520815-5 (detained by CBP in Tacoma).

15 **VIII. CBP Observations/Findings on Entry Summary Packages**

16 17. I examined the Entry Summary Packages for the vehicles listed above.  
17 Most are Kei vehicles. Cox purchased all 20 vehicles from Be Forward Co., Ltd.  
18 According to Be Forward's website, <https://www.beforward.jp/about>, "this company was  
19 among the first in Japan to offer online shopping of used cars for international export.  
20 With its cross-border ecommerce site developed exclusively for the firm, the company  
21 entered into the global ecommerce business market, selling and exporting used cars."

22 18. I also interviewed CBP Officer Jarrett Henderson on November 6, 2019.  
23 Officer Henderson is familiar with the documentation that must accompany cars imported  
24 into the United States. He spotted many unusual aspects in the Customs Entry Summary  
25 packages on the Kei cars imported by COX (listed in paragraph 15 above). For example,  
26 Henderson told me and showed me how COX claimed the vehicles all conformed to the  
27 United States Federal Motor Vehicle Safety Standards (FMVSS), and how COX had  
28

1 provided documents "certifying" their conformity to EPA and FMVSS standards.  
2 Somehow, however, though the cars came from several different manufacturers, the very  
3 same signature (i.e., the same person) appeared repeatedly on the FMVSS conformity  
4 certifications. The same person obviously did not sign each of these conformity  
5 certifications. If the signatures were false, then the certificates of conformity we falsely  
6 associated with the cars COX was importing.

7 19. In addition, Officer Henderson pointed out that many of the submitted  
8 certificates displayed that the ignition timing on the imported vehicle was "15%  
9 B.T.D.C.," even though the vehicles came from multiple manufacturers, had dissimilar  
10 engines, and dissimilar engine families and different manufacturers. It is very unlikely  
11 that all the cars would have the same ignition timing. More concerning, however, is that  
12 ignition timing is typically documented in degrees behind or ahead of top dead center, not  
13 in percentages. No manufacturer I know of uses percentages. The consistent  
14 reoccurrence of this unusual statement is therefore highly suspicious.

15 20. Officer Henderson also noted how the stamps on the certificates of  
16 conformity, showing they had been "approved," appeared to be fraudulent. For example,  
17 on the Mitsubishi certificates of conformity, a Russian "GOST R" stamp was used. The  
18 "GOST R" stamp is used to certify a commodity as conforming to the Eurasian Customs  
19 Union standards. The American arm of Mitsubishi would not use this stamp to certify  
20 that one of their cars met American standards.

21 21. Officer Henderson also pointed out how the certificates of conformity for  
22 the Honda vehicles listed above used a stamp/signature from a garage in India. A search  
23 of the internet uncovered a copy of the exact stamp/signature on a promotional letter from  
24 Apex Honda of India, a garage/workshop. Honda of America would not have used an  
25 Indian stamp on one of their Kei cars to certify conformity.

26 22. Officer Henderson also pointed out an anomaly on the documents for the  
27 BMW listed above. The contact information and signature on the conformity certificate  
28

1 submitted by COX for the BMW appeared to be taken from a letter, posted online by a  
2 BMW executive based in South Africa. The anomalous BMW documents show that the  
3 signature is cut off after the first letter, indicating that the signature from the South  
4 African letter had been copied and applied to the documents being submitted by  
5 CHRISTOPHER COX.

6 23. The certificate submitted for the entry documents for the Toyota listed  
7 above bear a signature from a Toyota executive based in London. The signature appears  
8 to have been copied from a letter that was published online. A Toyota executive in  
9 London would not have signed a certificate of conformity for a vehicle being imported  
10 into the United States.

11 24. The certificates for the Subarus listed above all have Be Forward's  
12 company stamp on them. However, the CEO's signature is cut off and shows only the  
13 last two characters.

14 25. On November 6, 2019, I spoke to CBP Officers Jarrett Henderson and Sara  
15 Cobb regarding two vehicles they had detained at the Port of Tacoma. They had spoken  
16 with CRISTOPHER COX on October 29, 2019. COX told them he had previously  
17 imported one vehicle from Canada, entering at the land border crossing in Montana.  
18 COX stated he drove the vehicle across the border with his father. COX said he knew an  
19 unidentified female who worked for the Washington Department of Licensing who  
20 helped him with vehicle registration paperwork. COX claimed he had an employment  
21 contract that required vehicles newer than 15 years, within specific guidelines. COX also  
22 stated that all the documents, except forms from the EPA and DOT, were sent to him  
23 from Be Forward Co. Ltd.

24 26. Officers Cobb and Henderson told me that CHRISTOPHER COX  
25 identified himself to them as a contract mail carrier for the United States Postal Service.  
26 COX showed them a Transportation Worker Identification Credential (TWIC) card.  
27 According to the Transportation Security Administration (TSA) official website, "the  
28



1 TWIC card is required by the Maritime Transportation Security Act for workers who  
 2 need access to secure areas of the nation's maritime facilities and vessels. TSA conducts  
 3 a security threat assessment (background check) to determine a person's eligibility and  
 4 issues the credential. U.S. citizens and immigrants in certain immigration categories may  
 5 apply for the credential."

6 27. On November 12, 2019, I spoke to Inspector Amy Kerkof of the United  
 7 States Postal Inspection Service (USPIS). Inspector Kerkof told me that  
 8 CHRISTOPHER COX was a Highway Contract Routes (HCR) Driver for the U.S. Postal  
 9 Service, and that he held an HCR contract for the area with zip code 98581. I was  
 10 informed that CHRISTOPHER COX's wife, Teresa Cox, was also an HCR driver for the  
 11 U.S. Postal Service, and that she held an HCR contract for the area within the zip code of  
 12 98590. I also reached out to TSA's representative, who provided me CHRISTOPHER  
 13 COX's TWIC card application. On the application, CHRISTOPHER COX stated that he  
 14 was employed by the United States Postal Service. The U.S. Postal Service neither  
 15 employed nor contracted COX to purchase vehicles, nor was he required to enter the Port  
 16 as any part of his contract to deliver mail.

17 **IX. Vehicles Seized in Tacoma: 2000 White Daihatsu Atrai Wagon VIN # S220G-**  
 18 **0016550, Entry # BMG-0520816-3 and 2007 White Mazda Bongo Van VIN**  
 19 **SK82V-322838, Entry # BMG-0520815-5**

20 28. On September 9, 2019, Sound Brokerage Intl. LLC. filed entry summaries  
 21 on behalf of CHRISTOPHER COX to import a 2000 White Daihatsu Atrai Wagon and a  
 22 2007 White Mazda Bongo Van (listed above and referred to now as the subject vehicles).  
 23 COX submitted a DOT Form HS-7, "Declaration Importation of Motor Vehicles and  
 24 Motor Vehicle Equipment Subject to Federal Motor Vehicle Safety, Bumper and Theft  
 25 Prevention Standards," for each subject vehicle. COX checked box number 2A in the  
 26 Form HS-7, which affirmed the following:  
 27  
 28

1 "The vehicle was certified by its original manufacturer as conforming to all  
2 applicable Canadian motor vehicle safety standards and its original manufacturer  
3 confirms that the vehicle conforms to all applicable U.S. Federal Motor Vehicle  
4 Safety, Bumper, and Theft Prevention Standards (or that it conforms to all such  
5 standards except for the labeling requirements of Standards Nos. 101 and 110 or  
6 120, and/or the specifications of Standard No. 108 relating to daytime running  
7 lamps), and the vehicle is not a salvage motor vehicle, a repaired salvage motor  
8 vehicle, or a reconstructed motor vehicle, and I am importing it for personal use.  
9 [591.5(g)];"

10 29. On September 24, 2019, CBP Officer Sara Cobb reached out to the DOT-  
11 National Highway Traffic Safety Administration (NHTSA) to request its opinion on  
12 whether the importation of the subject vehicles would be in compliance with the statutes  
13 and regulations administered by the NHTSA. NHTSA is the agency within the DOT  
14 responsible for improving safety on the nation's highways. To achieve this goal, NHTSA  
15 develops and enforces the Federal Motor Vehicle Safety Standards (FMVSS) discussed  
16 above, which requires minimum levels of safety performance for motor vehicles and  
17 equipment imported into the United States.

18 30. On September 30, 2019, DOT-NHTSA investigator Larry Hall responded  
19 to Officer Cobb and stated that NHTSA deemed the subject vehicles ineligible for  
20 importation. Investigator Larry Hall stated, "Mazda USA has confirmed that no Bongo  
21 Vans have ever been imported for sale in the U.S., nor have any of the Bongo Van  
22 vehicles ever been built to U.S. standards. Daihatsu, a wholly owned subsidiary of  
23 Toyota, has not built a U.S. spec vehicle since 1992. Therefore, importation of the  
24 subject vehicles would violate Title 49 United States Code § 30112(a)(1). Because Title  
25 49 United States Code § 30112(a)(1) is a law that relates to safety, and the subject vehicle  
26 does not comply with that law, we are of the opinion that CBP may seize (or deny entry)  
27 to the subject vehicle, and NHTSA would not be opposed to such an action."  
28

1 31. CHRISTOPHER COX also attached to the entry packages for the subject  
2 vehicles EPA form 3520-1 "Declaration Form Importation of Motor Vehicles and Motor  
3 Vehicle Engines Subject to Federal Air Pollution Regulations." On this form, code EE  
4 was checked in the affirmative, and it stated the following:

5 "Identical in all material respects to a U.S. certified version - either 1) Canadian  
6 vehicle (proof required e.g. Canadian emission control label, registration or title,  
7 or letter from the U.S. or Canadian manufacturer representative on letterhead  
8 verifying manufacture for sale in Canada) or 2) vehicle from any country with  
9 letter attached to this form from the manufacturer's U.S. representative on  
10 letterhead (not a dealer or mechanic) stating that the vehicle is identical to a U.S.  
11 EPA certified version with respect to emissions. The importer attests that vehicle  
12 is being imported for purposes other than resale or lease. For import of "identical"  
13 Canadian vehicles for resale, use code FF."

14 32. On September 23, 2019, CBP Officer Cobb reached out to the EPA and  
15 requested its opinion on whether the importation of the subject vehicles would in fact be  
16 in compliance with the Clean Air Act (hereinafter referred as Act). On October 16, 2019,  
17 EPA responded to CBP and stated the following:

18 "The importer claimed box "EE" on EPA's Declaration Form 3520-1 for each  
19 subject vehicle. This provision applies to vehicles from countries other than  
20 Canada where the application is accompanied by a letter from the vehicle's  
21 manufacturer's U.S. representative on letterhead stating that the vehicle is identical  
22 to a U.S. EPA certified version with respect to emissions and where the importer  
23 attests that the vehicle is being imported for purposes other than resale or lease.

24 33. Neither COX nor the customs agent he used had provided such a letter for  
25 either vehicle (i.e., from the vehicle's manufacturer's U.S. representative on letterhead  
26 stating that the vehicle is identical to a U.S. EPA certified version with respect to  
27 emissions). Additionally, a review of EPA's database found no certified vehicles with  
28



1 specifications consistent with the subject vehicles. The EPA determined that the subject  
 2 vehicles were not certified, and no facts demonstrate eligibility for any exemption or  
 3 exclusion. Thus, by importing the subject vehicles, the importer committed violations of  
 4 the Clean Air Act's statutory and regulatory provisions. The EPA therefore recommended  
 5 that CBP seize, export or otherwise deny entry.

6 **X. Importation of Used 2001 Honda Vamos, VIN # HM21204538, Entry # BMG-**  
 7 **0519661-6**

8 34. On January 11, 2019, Sound Brokerage Intl. LLC. filed an entry summary  
 9 with CBP on behalf of CHRISTOPHER COX to import a 2001 Silver Honda Vamos  
 10 Passenger Van, VIN # HM21204538, Entry # BMG-059661-6 (hereinafter referred as the  
 11 Honda Vamos). The entry summary package contained Customs Entry forms, and other  
 12 forms, including DOT form HS-7 (Declaration Importation of Motor Vehicles and Motor  
 13 Vehicle Equipment Subject to Federal Motor Vehicle Safety, Bumper and Theft  
 14 Prevention Standards). The package also included EPA form 3520-1 (Declaration Form  
 15 Importation of Motor Vehicles and Motor Vehicle Engines Subject to Federal Air  
 16 Pollution Regulations).

17 35. On November 22, 2019, I reached out to the National Highway Traffic  
 18 Safety Administration (NHTSA) and the EPA to request evaluation of the safety and  
 19 environmental compliance of the subject vehicle. On November 25, 2019, NHTSA  
 20 responded to my request and stated that the vehicle could not be imported because it "was  
 21 not certified by its original manufacturer as conforming to all applicable Canadian motor  
 22 vehicle safety standards and its original manufacturer confirms that the vehicle conforms  
 23 to all applicable U.S. Federal Motor Safety, Bumper, and Theft Prevention Standards (or  
 24 that it conforms to all such standards except for the labeling requirements of Standards  
 25 Nos. 101 and 110 or 120, and/or the specifications of Standard No. 108 relating to  
 26 daytime running lamps), and the vehicle is not a salvage motor vehicle, a repaired salvage  
 27 motor vehicle, or a reconstructed motor vehicle, and I am importing it for personal use."  
 28

1 NHTSA further stated that importation of the subject vehicle would violate Title 49  
2 U.S.C. § 30112(a)(1). NHTSA recommended the Honda Vamos be seized.

3 36. On December 4, 2019, the EPA responded to my request and stated that the  
4 EPA Declaration Form 3520-21, provided by CHRISTOPHER COX, selected Code EE  
5 as identical in all material respects to the United States certified version - either 1)  
6 Canadian vehicle (proof required e.g. Canadian emission control label, registration or  
7 title, or letter from the U.S. or Canadian manufacturer representative on letterhead  
8 verifying manufacture for sale in Canada) or 2) vehicle from any country with letter  
9 attached to this form from the manufacturer of the United States representative on  
10 letterhead (not a dealer or mechanic) stating that the vehicle is identical to a United States  
11 made - EPA certified version with respect to emissions.

12 37. In fact, because the Honda Vamos was not a Canadian made vehicle, it  
13 required a letter from the manufacturer of the United States representative on letterhead  
14 (not a dealer or mechanic) stating that the vehicle is identical to a United States made -  
15 EPA certified version with respect to emissions. However, COX did not provide this  
16 letter. Instead, he provided a document purporting to be a "certificate of conformity."

17 38. In addition, EPA personnel searched EPA's certification database and were  
18 unable to identify any vehicle that matched the specifications of the Honda Vamos.  
19 Specifically, EPA personnel found no certificates of conformity issued to Honda for the  
20 2001 model year that had 650 cc engines. Based on this finding, EPA personnel  
21 concluded that CHRISTOPHER COX could not have obtained the letter required by  
22 Code EE because the vehicle was not in fact identical to any U.S. EPA certified version.

23 39. By selecting code EE, COX attested that the Honda Vamos was being  
24 imported for purposes other than resale or lease. According to the Washington State  
25 Department of Licensing, however, on January 16, 2019, COX sold the subject vehicle to  
26 WRC, of Dupont, WA. According to records, the Honda Vamos was reportedly sold for  
27 \$381.00 USD. WRC then registered the Honda Vamos with Washington State  
28

1 Department of Licensing – Port Orchard License Agency--on the same date. The subject  
2 vehicle was issued license plates BNF9080.

3 40. After further review of the entry package, I observed the U.S. Department  
4 of Homeland Security's seal was stamped on two CBP forms: CBP Form 7501 "Entry  
5 Summary" and CBP Form 3461 "Entry/Immediate Delivery." I compared the seal to the  
6 true U.S. Department of Homeland Security's seal, it appeared that CHRISTOPHER  
7 COX forged the U.S. Department of Homeland Security seal and stamped it on the CBP's  
8 documents. I also spoke to CBP Officer Henderson about the seal. Officer Henderson  
9 stated that he believed that the U.S. Department of Homeland Security seal stamped on  
10 both CBP forms was forged. Officer Henderson stated that he stamped the real U.S.  
11 Department of Homeland Security seal on paper, made a copy of the paper, then  
12 compared it to the U.S. Department of Homeland Security seal on both CBP forms  
13 mentioned above. Officer Henderson concluded that the U.S. Department of Homeland  
14 Security seal on each form was forged. Officer Henderson stated that the real U.S.  
15 Department of Homeland Security seal would have officer's badge number and his or her  
16 signature on it.

17 **XI. Surveillance at COX Residence and Importation of 1994 Subaru KS4 Flatbed**  
18 **Truck with VIN # KS4188364**

19 41. On November 14, 2019, I conducted surveillance at COX's residence at  
20 1051 NE Belfair Manor Dr., Belfair, WA. According to the Mason County Assessor's  
21 Office, CHRISTOPHER COX is the owner of the property. According to the  
22 Washington State Department of Licensing, CHRISTOPHER COX resides at this  
23 property. I observed many vehicles at the residence. I and checked and confirmed that  
24 they were registered to CHRISTOPHER COX and his wife Teresa Cox. I saw a white  
25 truck with a camper top attached to it, with Washington license plates C40125P. A  
26 record check confirmed the vehicle is registered to CHRISTOPHER COX at 1051 NE  
27  
28



1 Belfair Manor Dr., Belfair, WA. The vehicle was registered as a white 1994 Subaru KS4  
2 flatbed truck with VIN # KS4188364, also known as Subaru Sambar.

3 42. I conducted record checks with the U.S. Homeland Security database and  
4 Washington State Department of Licensing on the Subaru Sambar and determined the  
5 following. On May 17, 2019, Sound Brokerage Intl. LLC. filed entry summaries with  
6 CBP on behalf of CHRISTOPHER COX to import the 1994 Subaru Sambar V-KS4  
7 flatbed truck, VIN # KS4 188364, entry number BMG-0520177-0 (hereinafter referred as  
8 the Sambar truck). Attached to the entry packages, CHRISTOPHER COX submitted  
9 DOT Form HS-7, "Declaration Importation of Motor Vehicles and Motor Vehicle  
10 Equipment Subject to Federal Motor Vehicle Safety, Bumper and Theft Prevention  
11 Standards." CHRISTOPHER COX checked box number 1, which stated "the vehicle is  
12 25 or more years old or the equipment item was manufactured on a date when no  
13 applicable Federal Motor Vehicle Safety Standard or Theft Prevention Standard was in  
14 effect. Date of manufacture: 12/05/1993 [591.5(i)]" All this appears to be true, which I  
15 believe shows that COX knows the correct way to complete the DOT form.

16 43. CHRISTOPHER COX also attached to the entry package EPA form 3520-1  
17 "Declaration Form Importation of Motor Vehicles and Motor Vehicle Engines Subject to  
18 Federal Air Pollution Regulations." On this form, code E under section of "EPA  
19 exempted vehicles" was checked, and it stated "vehicle at least 21 years old (calendar  
20 year of manufacture subtracted from year of importation) and in original unmodified  
21 configuration is either exempted or excluded from EPA emission requirements,  
22 depending on age. Vehicles at least 21 years old with replacement engines are not  
23 eligible for this exemption unless they contain equivalent or newer EPA certified engines.  
24 Customs may require proof of vehicle age." Again, this appears to be a true and correct  
25 entry on the EPA form by COX.

26 44. On May 22, 2019, the Sambar truck was registered with Washington State  
27 Department of Licensing. The subject vehicle was issued license plates C40125P.  
28

1       45. After further review of the entry package, I observed the U.S. Department  
2 of Homeland Security's seal was stamped on two CBP forms: CBP Form 7501 "Entry  
3 Summary" and CBP Form 3461 "Entry/Immediate Delivery." I compared these two  
4 stamped forms to the true U.S. Department of Homeland Security's seal. To me, it  
5 appears that CHRISTOPHER COX forged the U.S. Department of Homeland Security  
6 seal and stamped it onto the importation/customs entry documents. CBP would have  
7 stamped the forms when they performed the mandatory inspections of the vehicles. If the  
8 forms are not stamped, COX runs the risk of being unable to register the vehicle in the  
9 State of Washington. Accordingly, it appears that COX evaded CBP inspection and  
10 instead applied a counterfeit stamp, thus increasing the chances that the car would be  
11 accepted for registration.

12       46. On November 27, 2019, I consulted with CBP regarding CHRISTOPHER  
13 COX's entry summary package on the Sambar truck. It appeared to CBP that  
14 CHRISTOPHER COX checked the correct boxes on the EPA and DOT Forms. It  
15 appeared that the 1994 Subaru Sambar V-KS4 flatbed truck was purchased in April 2019  
16 and arrived in the United States in May 2019. The Sambar truck thus met the age  
17 exemptions for DOT and EPA. On the EPA Form 3520-1, box E was checked, correctly  
18 indicating the Sambar truck was at least 21 years of age. On the DOT Form HS-7, box 1  
19 was checked, correctly indicating the Samar truck was at least 25 years of age.  
20 Therefore, the subject vehicle was legally imported into the United States in May 2019.  
21 However, the counterfeit stamps imply that COX illegally removed the truck from the  
22 port without proper inspection.  
23  
24  
25  
26  
27  
28

**XII. Interviews of Employee and Owner of Sound Brokerage**

47. COX used "Sound Brokerage," a customs agent, to assist in the importation of all the vehicles discussed in this affidavit. On November 22, 2019, I interviewed Mandee Compton of Sound Brokerage at her office at 3600 Port of Tacoma Road, Suite # 301, Tacoma, WA. Ms. Compton provided me with information on the general procedures Sound Brokerage followed to import a vehicle. Ms. Compton stated that Sound Brokerage was a small company and that the owner was Gwen Salisbury. Part of Sound Brokerage's business was vehicle importation. Sound Brokerage was more or less a "middle man," acting on behalf of the importers (like COX). Sound Brokerage is licensed/certified with CBP to file all import/export documents for its customers.

48. If an importer wanted to use the services of Sound Brokerage to import a vehicle, he/she needed to sign a "Customs Power of Attorney," which allowed Sound Brokerage to act on the importer's behalf. The importer had to provide Sound Brokerage an invoice for the vehicle, the DOT form HS-7 ("Declaration Importation of Motor Vehicles and Motor Vehicle Equipment Subject to Federal Motor Vehicle Safety, Bumper and Theft Prevention Standards"), and the EPA form 3520-1 ("Declaration Form Importation of Motor Vehicles and Motor Vehicle Engines Subject to Federal Air Pollution Regulations.") The importer also had to provide the Bill of Lading, and any other forms required by other federal agencies. Ms. Compton stated that all the forms had to be filled out by the importer. Neither she nor other personnel from Sound Brokerage ever filled out the forms.

49. After gathering all necessary documents, Sound Brokerage would enter information into Automated Commercial Environment (ACE), a computer/internet-based cargo release and entry summary processing system owned by CBP. ACE would then generate two CBP forms, Form 7501 "Entry Summary," and Form 3461 "Entry/Immediate Delivery." Sound Brokerage personnel would then upload all the forms and documents to Document Image System (DIS), another computer/internet-based



1 cargo release system owned by CBP. Within hours, ACE-DIS would let Sound  
2 Brokerage know if the vehicle was cleared/ready to be released/picked up. To my  
3 knowledge, ACE-DIS is an automated clearance system. Unless the vehicle/shipment  
4 was marked with certain codes and/or flagged by CBP, the vehicle/shipment would be  
5 automatically approved and released.

6 50. Once the vehicle was cleared and ready for pick up, Sound Brokerage  
7 would notify the importer. Sound Brokerage would provide him or her all the  
8 commercial documents originally sent by the importer, and any newly created documents  
9 from the ACE-DIS system. The importer would then take all the documents to the East  
10 Blair 1 Terminal (EB1), 2940 East Alexander Avenue, Tacoma, WA to pick up the  
11 vehicle. Ms. Compton stated that Sound Brokerage would always remind the importer to  
12 take all the documents and the vehicle to the CBP office for inspection. Ms. Compton  
13 provided me copies of several documents that instructed the importer to take the  
14 documents and the vehicle to the CBP office for inspections. One document even  
15 included a map of the Port of Tacoma area showing the EB1 terminal and the CBP office.

16 51. On the same day I interviewed Ms. Compton, I also interviewed Gwen  
17 Salisbury of Sound Brokerage. Ms. Salisbury reaffirmed Ms. Compton's statement on  
18 general procedure of Sound Brokerage for importation of vehicles. Ms. Salisbury has  
19 approximately 40 years-experience as a customs broker. She has owned and operated  
20 Sound Brokerage since 2003. She met CHRISTOPHER COX in November 2017, but  
21 could not remember how COX was referred to Sound Brokerage. She showed me  
22 documents for the first vehicle COX imported into the United States with the use of her  
23 firm: a 2004 Suzuki Jimny. It was imported on November 29, 2017. Since then, since  
24 then, Sound Brokerage helped CHRISTOPHER COX import approximately 24 vehicles.

25 52. Ms. Salisbury remembered that she had escorted CHRISTOPHER COX to  
26 pick up the vehicle at EB1 terminal several times. She stated that COX did not have a  
27 Transportation Worker Identification Credential (TWIC card) back then. After escorting  
28

1 CHRISTOPHER COX to the terminal to pick up the vehicles on multiple occasions, Ms.  
2 Salisbury provided CHRISTOPHER COX directions on how to obtain a TWIC card,  
3 which he did.

4 53. Ms. Salisbury stated that she never picked up vehicles on CHRISTOPHER  
5 COX's behalf. She understood from CHRISTOPHER COX was employed by the United  
6 States Postal Service (USPS), in part because she saw him walking into her office with a  
7 USPS identification card. CHRISTOPHER COX told her he needed the vehicles for his  
8 job at the Post Office.

9 54. Ms. Salisbury reiterated that she told all her customers to bring their import  
10 documents and the vehicle to the CBP office for inspection. She understood that CBP  
11 Officers needed to stamp the CBP Form 3461 "Entry/Immediate Delivery," so the vehicle  
12 could be registered with Washington State Department of Licensing. She advised  
13 CHRISTOPHER COX to bring the vehicle to CBP every time she notified him a vehicle  
14 was releasing/ready for pick up.

15 55. Ms. Salisbury stated that COX usually sent his importation package to her  
16 by email. If she needed anything from him, Ms. Salisbury would email or send COX a  
17 text message. Ms. Salisbury confirmed that CHRISTOPHER COX used his email  
18 account cctc53611@gmail.com to communicate with her.

19 **XIII. Probable Cause that Email Account cctc53611@gmail.com**  
20 **contains Information Concerning criminal activity**

21 56. I have reviewed Customs Entry Summary packages for the Kei vehicles  
22 imported by CHRISTOPHER COX. I observed that COX used his email account  
23 (cctc53611@gmail.com) to email and transmit documents regarding his Customs Entry  
24 Summary packages. For instance, on the Invoice/Bill of Sale form from Be Forward Co.  
25 Ltd., found in the Customs Entry Summary package for vehicle # 1 - Used 2007 Honda  
26 Odysse, COX used his email account cctc53611@gmail.com to place the original orders  
27 from Be Forward. COX also listed cctc53611@gmail.com as his email address, and  
28

1 included his correct mailing address and cellular phone number in his contact  
2 information.

3 57. I also reviewed several documents entitled "Bill of Lading," included in the  
4 Customs Entry Summary packages. On these documents, COX listed his name, address,  
5 telephone number, and email account (cctc53611@gmail.com) under the "consignee"  
6 section of the document.

7 58. On December 18, 2019 I reviewed several email communications between  
8 Ms. Salisbury and COX, where COX used email account cctc53611@gmail.com. The  
9 emails discussed the importation of vehicles. COX also used email account  
10 cctc53611@gmail.com to attach/send/receive documents to/from Ms. Salisbury. For  
11 instance, in an email dated December 31, 2018 at 1:10 AM, COX sent an email to Gwen  
12 Salisbury regarding the importation of the used 2001 Honda Vamos, VIN#  
13 HM21204538, entry date January 11, 2019, and entry # BMG-0519661-6 (Vehicle # 12).  
14 On this email, COX attached the DOT form, EPA form, Export Certificate, Order Form  
15 from Be Forward, and Certificate of Conformity.

16 59. It appears that COX used cctc53611@gmail.com to communicate with Be  
17 Forward. As stated above, this email account appeared on documents generated by Be  
18 Forward (for example, Invoice/Bill of Sale.) It is likely then that the contents of  
19 cctc53611@gmail.com will contain copies of the original, unaltered documents COX  
20 obtained from Be Forward.

#### 21 **XIV. Background Concerning Online Accounts**

22 60. As explained herein, information stored in connection with an online  
23 account may provide crucial evidence of the "who, what, why, when, where, and how" of  
24 the criminal conduct under investigation, thus enabling the United States to establish and  
25 prove each element or alternatively, to exclude the innocent from further suspicion.

26 61. In my training and experience, the information stored in connection with an  
27 online account can indicate who has used or controlled the account. This "user  
28



1 attribution" evidence is analogous to the search for "indicia of occupancy" while  
2 executing a search warrant at a residence. For example, email communications, contacts  
3 lists, and images sent (and the data associated with the foregoing, such as date and time)  
4 may indicate who used or controlled the account at a relevant time.

5 62. Further, information maintained by the email provider can show how and  
6 when the account was accessed or used. For example, as described below, email  
7 providers typically log the Internet Protocol (IP) addresses from which users access the  
8 email account, along with the time and date of that access. By determining the physical  
9 location associated with the logged IP addresses, investigators can understand the  
10 chronological and geographic context of the email account access and use relating to the  
11 crime under investigation. This geographic and timeline information may tend to either  
12 inculcate or exculpate the account owner. Additionally, information stored at the user's  
13 account may further indicate the geographic location of the account user at a particular  
14 time (e.g., location information integrated into an image or video sent via email).

15 63. Stored electronic data may provide relevant insight into the email account  
16 owner's state of mind as it relates to the offense under investigation. For example,  
17 information in the email account may indicate the owner's motive and intent to commit a  
18 crime (e.g., communications relating to the crime), or consciousness of guilt (e.g.,  
19 deleting communications in an effort to conceal them from law enforcement).

## 20 **XV. Technical Background**

21 64. I have learned that Google provides a variety of on-line services, including  
22 electronic mail (email) access, to the general public. Google allows subscribers to obtain  
23 e-mail accounts at the domain name "gmail.com," like the email accounts listed in  
24 Attachment A.

25 65. Subscribers obtain an account by registering with Google. When doing so,  
26 email providers like Google ask the subscriber to provide certain personal identifying  
27  
28

1 information. This information can include the subscriber's full name, physical address,  
2 telephone numbers and other identifiers, alternative email addresses, and, for paying  
3 subscribers, means and source of payment (including any credit or bank account number).  
4 In my training and experience, such information may constitute evidence of the crimes  
5 under investigation because the information can be used to identify the account's user or  
6 users, and to help establish who has dominion and control over the account.

7 66. Email providers typically retain certain transactional information about the  
8 creation and use of each account on their systems. This information can include the date  
9 on which the account was created, the length of service, records of log-in (i.e., session)  
10 times and durations, the types of service utilized, the status of the account (including  
11 whether the account is inactive or closed), the methods used to connect to the account  
12 (such as logging into the account via Google's website), and other log files that reflect  
13 usage of the account. In addition, email providers often have records of the Internet  
14 Protocol address ("IP address") used to register the account and the IP addresses  
15 associated with particular logins to the account. Because every device that connects to  
16 the Internet must use an IP address, IP address information can help to identify which  
17 computers or other devices were used to access the email account, which can help  
18 establish the individual or individuals who had dominion and control over the account

19 67. In general, an email that is sent to a Google subscriber is stored in the  
20 subscriber's "mail box" on Google's servers until the subscriber deletes the email. If the  
21 subscriber does not delete the message, the message can remain on Google's servers  
22 indefinitely. Even if the subscriber deletes the email, it may continue to be available on  
23 Google's servers for a certain period of time.

24 68. When the subscriber sends an email, it is initiated at the user's computer,  
25 transferred via the Internet to Google's servers, and then transmitted to its end  
26 destination. Google often maintains a copy of the email sent. Unless the sender of the  
27 email specifically deletes the email from the Google server, the email can remain on the  
28

1 system indefinitely. Even if the sender deletes the email, it may continue to be available  
2 on Google's servers for a certain period of time.

3 69. A sent or received email typically includes the content of the message,  
4 source and destination addresses, the date and time at which the email was sent, and the  
5 size and length of the email. If an email user writes a draft message but does not send it,  
6 that message may also be saved by Google but may not include all of these categories of  
7 data.

8 70. A Google subscriber can also store files, including emails, address books,  
9 contact or buddy lists, calendar data, photographs, and other files, on servers maintained  
10 and/or owned by Google. In my training and experience, evidence of who was using an  
11 email account may be found in address books, contact or buddy lists, email in the  
12 account, attachments to emails, including photographs and files, and photographs and  
13 files stored in relation to the account.

14 71. A subscriber to a Google Gmail account can also store files, including  
15 address books, contact lists, calendar data, photographs and other files, on servers  
16 maintained and/or owned by Google. For example, Google offers users a calendar  
17 service that users may utilize to organize their schedule and share events with others.  
18 Google also offers users' a service called Google Drive that may be used to store data and  
19 documents. The Google Drive service may be used to store documents including  
20 spreadsheets, written documents (such as Word or Word Perfect) and other documents  
21 that could be used to manage a website. Google Drive allows users to share their  
22 documents with others or the public depending on the settings selected by the account  
23 holder. Google also provides its users with access to the photo storage service "Google +  
24 Photos," formerly known as Picasa. Google + Photos can be used to create photo  
25 albums, store photographs, and share photographs with others. Another Google service  
26 called "You Tube" allows users to view, store and share videos. Google also provides a  
27 service called "Google Analytics." Google Analytics is a Google service that monitors  
28



1 website traffic and provides subscribers with data relating to how much traffic is visiting  
2 the subscriber's website, which sections of the subscriber's website users are visiting,  
3 how long users are staying on particular sections of the site, and the geographical source  
4 of users visiting the website, among other things. Another Google service called "Google  
5 Hangouts" is a communication platform which includes instant messaging, video chat,  
6 short message service (SMS) and voice over internet protocols (VOIP) features.

7 72. In some cases, email account users will communicate directly with an email  
8 service provider about issues relating to the account, such as technical problems, billing  
9 inquiries, or complaints from other users. Email providers typically retain records about  
10 such communications, including records of contacts between the user and the provider's  
11 support services, as well records of any actions taken by the provider or user as a result of  
12 the communications. In my training and experience, such information may constitute  
13 evidence of the crimes under investigation because the information can be used to  
14 identify the account's user or users.

15 **XVI. Information To Be Searched And Items To Be Seized**

16 73. Pursuant to Title 18, United States Code, Section 2703(g), this application  
17 and affidavit for a search warrant seeks authorization to permit Google and its  
18 representatives and employees to assist agents in the execution of the warrant. Once  
19 issued, the search warrant will be presented to Google with direction that the company  
20 identify the account described in the specific Attachment A as well as other subscriber  
21 and log records associated with the Gmail account as set forth in the specific Attachment  
22 B.

23 74. The search warrants will direct Google to create an exact copy of the  
24 specified account and records.

25 75. I, and/or other law enforcement personnel will thereafter review the copy of  
26 the electronically stored data and identify from among that content those items that come  
27 within the items identified in Section II to the applicable Attachment B, for seizure.  
28

1       76. Analyzing the data contained in the forensic image may require special  
2 technical skills, equipment, and software. It could also be very time-consuming.  
3 Searching by keywords, for example, can yield thousands of "hits," each of which must  
4 then be reviewed in context by the examiner to determine whether the data is within the  
5 scope of the warrant. Merely finding a relevant "hit" does not end the review process.  
6 Keywords used originally need to be modified continuously, based on interim results.  
7 Certain file formats, moreover, do not lend themselves to keyword searches, as keywords,  
8 search text, and many common email, database and spreadsheet applications do not store  
9 data as searchable text. The data may be saved, instead, in proprietary non-text format.  
10 And, as the volume of storage allotted by service providers increases, the time it takes to  
11 properly analyze recovered data increases, as well. Consistent with the foregoing,  
12 searching the recovered data for the information subject to seizure pursuant to this  
13 warrant may require a range of data analysis techniques and may take weeks or even  
14 months. All forensic analysis of the data will employ only those search protocols and  
15 methodologies reasonably designed to identify and seize the items identified in Section II  
16 of Attachment B to the warrant.

17       77. Based on my experience and training, and the experience and training of  
18 other agents with whom I have communicated, it is necessary to review and seize a  
19 variety of messenger communications, chat logs, files, payment records and documents,  
20 that identify any users of the subject account and communications sent or received in  
21 temporal proximity to incriminating messages that provide context to the incriminating  
22 communications.

### 23                   **XVII. Sealing Request**

24       78. It is respectfully requested that the Court issue an order sealing, until  
25 further order of the Court, all papers submitted in support of the requested warrants,  
26 including the application, this affidavit, the attachments, and the requested warrants. I  
27 believe that sealing these documents is necessary because the information to be seized is  
28

1 relevant to an ongoing investigation and includes references to cooperating individuals.  
2 Premature disclosure of the contents of the application, this affidavit, the attachments,  
3 and the requested warrants may adversely affect the integrity of the investigation,  
4 including giving targets a chance to destroy evidence or take other steps to hinder the  
5 investigation.

#### 6 **XVIV. Non Disclosure Request**

7 79. The United States requests that the Court order Google Inc. refrain from  
8 notifying any person (including the subscribers and customers of the accounts) listed in  
9 the warrant of the existence of the attached warrant for one year.

10 80. Google Inc. is a provider of an electronic communication service, as  
11 defined in 18 U.S.C. § 2510(15), and/or a remote computing service, as defined in 18  
12 U.S.C. § 2711(2). Pursuant to 18 U.S.C. § 2703, the United States hopes to obtain the  
13 attached warrant, which will require Google Inc. to disclose certain records and  
14 information to the United States. This Court has authority under 18 U.S.C. § 2705(b) to  
15 issue "an order commanding a provider of electronic communications service or remote  
16 computing service to whom a warrant, subpoena, or court order is directed, for such  
17 period as the court deems appropriate, not to notify any other person of the existence of  
18 the warrant, subpoena, or court order."

19 81. In this case, such an order would be appropriate because the attached  
20 warrant relates to an ongoing criminal investigation that is neither public nor known to all  
21 the targets of the investigation, and its disclosure may alert the targets to the ongoing  
22 investigation. Accordingly, there is reason to believe that notification of the existence of  
23 the attached warrant will seriously jeopardize the investigation and alert people to  
24 conceal, tamper with, or destroy evidence. Some of the evidence in this investigation is  
25 stored electronically. If alerted to the existence of the warrant, the subjects under  
26 investigation could destroy that evidence, including information saved to their personal  
27 computers.



**XVIII. CONCLUSION**

82. Based on the information set forth herein, there is probable cause to search the above described email account cctc53611@gmail.com, as further described in Attachment A, for evidence, fruits and instrumentalities, as further described in Attachment B, of crimes committed by the individuals listed in this affidavit and their coconspirators specifically in violation of Title 18, United States Code, Sections 506 (Fraudulently using Seals of Department or Agencies) 545 (Smuggling Goods into the United States), 912 (Falsely Impersonating an Officer or Employee of the United States) 1001 (Making Material False Statements) 1036 (Making Entry to a Secure Area of a Seaport by False Pretenses) and 1343 (Committing Fraud by wire, radio, or television).

83. WHEREFORE, the United States respectfully requests that the Court issue the attached search warrant, and that it grant the attached Order directing Google Inc. not to disclose the existence or content of the attached warrant for one year, except that Google Inc. may disclose the attached warrant to an attorney for Google Inc for the purpose of receiving legal advice.

//

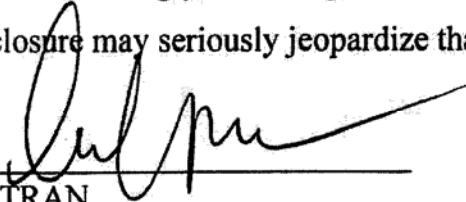
//

//

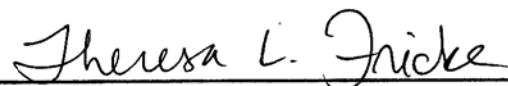
//

//

1       84.    The United States further requests that the Court order that this application  
2 and any resulting order be sealed until further order of the Court. As explained above,  
3 these documents discuss an ongoing criminal investigation that is neither public nor  
4 known to all of the targets of the investigation. Accordingly, there is good cause to seal  
5 these documents because their premature disclosure may seriously jeopardize that  
6 investigation.

7   
8 LY TRAN  
9 Special Agent  
Homeland Security Investigations

10       The above-named agent provided a sworn statement attesting to the truth of the  
11 contents of the foregoing affidavit on this 17<sup>th</sup> day of March, 2020.

12  
13   
14 THERESA L. FRICKE  
15 United States Magistrate Judge  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**ATTACHMENT A**

**SUBJECT ACCOUNT to be Searched**

The electronically stored data, information and communications contained in, related to, and associated with, including all preserved data associated with the Google account cctc53611@gmail.com, as well as all other subscriber and log records associated with the account, which is stored at premises owned, maintained, controlled, or operated by Google Inc., an electronic communications services and remote computing services provider located at 1600 Amphitheatre Parkway, Mountain View, California 94043.



**ATTACHMENT B****Section I - Information to be disclosed by Google for search:**

To the extent that the information described in Attachment A-1 is within the possession, custody, or control of Google, including any emails, records, files, logs, or information that has been deleted but is still available to Google. Google is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email, and any attachments to such emails;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, instant messages, and instant messenger contact information, calendar data, pictures, and files.

e. All records pertaining to communications between Google and any person regarding the account, including contacts with support services and records of actions taken.

**Section II - Information to be seized by the government**

All information described above in Section I that constitutes contraband, evidence, fruits, or instrumentalities of the following crimes committed on or after November 30, 2017: Title 18, United States Code, Section 506 – Seals of Department or Agencies, Title 18 United States Code, Section 545 – Smuggling Goods into the United States, Title 18 United States Code, Section 912 – Officer or Employee of the United States, Title 18 United States Code, Section 1001 False Statements, Title 18 United States Code Section 1036, Entry by False Pretenses to an real Property, Vessel, or Aircraft of the United States or Secure Area of any Airport or Seaport, and Title 18 United States Code, Section 1343 - Fraud by wire, radio, or television.

a. All messages, documents, and profile information, attachments, or other data that serves to identify any persons who use or access the account specified, or who exercise in any way any dominion or control over the specified account

b. Any address lists or “friend”/contact lists associated with the specified account;

c. All subscriber records associated with the specified account, including name, address, local and long distance telephone connection records, or records of session times and durations, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address, and means and source of payment for such service) including any credit card or bank account number;

d. Any and all other log records, including IP address captures, associated with the specified account;

e. Any records, documents, forms, attachments, photographs, and pictures relating to importation of vehicles and vehicle parts;

f. Any records and email communications to and from Be Forward Co. Ltd., and Sound Brokerage; and

1 g. Any records of communications between Google and any person about issues  
2 relating to the account, such as technical problems, billing inquiries, or complaints from  
3 other users about the specified account. This to include records of contacts between the  
4 subscriber and the provider's support services, as well as records of any actions taken by  
5 the provider or subscriber as a result of the communications.

6 Google is hereby ordered to disclose the above information to the government  
7 within 14 days of service of this warrant.  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28



## UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of )

(Briefly describe the property to be searched  
or identify the person by name and address) )INFORMATION ASSOCIATED WITH GOOGLE  
ACCOUNT cctc53611@gmail.com MORE FULLY  
DESCRIBED IN ATTACHMENT A. )Case No. MJ20-5061

## SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Northern District of California  
(identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A, ATTACHED HERETO AND INCORPORATED HEREIN BY REFERENCE.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

SEE ATTACHMENT B-1, ATTACHED HERETO AND INCORPORATED HEREIN BY REFERENCE.

YOU ARE COMMANDED to execute this warrant on or before March 31, 2020 (not to exceed 14 days)☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Any Magistrate Judge in the WDWA  
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for \_\_\_\_\_ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of \_\_\_\_\_Date and time issued: March 17, 2020  
1:35 PMTheresa L. Fricke  
Judge's signatureCity and state: Tacoma, Washington

Theresa L. Fricke, United States Magistrate Judge

Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

**Return**

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

**Certification**

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: \_\_\_\_\_

\_\_\_\_\_  
*Executing officer's signature*\_\_\_\_\_  
*Printed name and title*

**ATTACHMENT A**

**SUBJECT ACCOUNT to be Searched**

The electronically stored data, information and communications contained in, related to, and associated with, including all preserved data associated with the Google account cctc53611@gmail.com, as well as all other subscriber and log records associated with the account, which is stored at premises owned, maintained, controlled, or operated by Google Inc., an electronic communications services and remote computing services provider located at 1600 Amphitheatre Parkway, Mountain View, California 94043.



**ATTACHMENT B**

**Section I - Information to be disclosed by Google for search:**

To the extent that the information described in Attachment A-1 is within the possession, custody, or control of Google, including any emails, records, files, logs, or information that has been deleted but is still available to Google. Google is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email, and any attachments to such emails;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, instant messages, and instant messenger contact information, calendar data, pictures, and files.

e. All records pertaining to communications between Google and any person regarding the account, including contacts with support services and records of actions taken.

**Section II - Information to be seized by the government**

All information described above in Section I that constitutes contraband, evidence, fruits, or instrumentalities of the following crimes committed on or after November 30, 2017: Title 18, United States Code, Section 506 – Seals of Department or Agencies, Title 18 United States Code, Section 545 – Smuggling Goods into the United States, Title 18 United States Code, Section 912 – Officer or Employee of the United States, Title 18 United States Code, Section 1001 False Statements, Title 18 United States Code Section 1036, Entry by False Pretenses to an real Property, Vessel, or Aircraft of the United States or Secure Area of any Airport or Seaport, and Title 18 United States Code, Section 1343 - Fraud by wire, radio, or television.

a. All messages, documents, and profile information, attachments, or other data that serves to identify any persons who use or access the account specified, or who exercise in any way any dominion or control over the specified account

b. Any address lists or “friend”/contact lists associated with the specified account;

c. All subscriber records associated with the specified account, including name, address, local and long distance telephone connection records, or records of session times and durations, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address, and means and source of payment for such service) including any credit card or bank account number;

d. Any and all other log records, including IP address captures, associated with the specified account;

e. Any records, documents, forms, attachments, photographs, and pictures relating to importation of vehicles and vehicle parts;

f. Any records and email communications to and from Be Forward Co. Ltd., and Sound Brokerage; and

1 g. Any records of communications between Google and any person about issues  
2 relating to the account, such as technical problems, billing inquiries, or complaints from  
3 other users about the specified account. This to include records of contacts between the  
4 subscriber and the provider's support services, as well as records of any actions taken by  
5 the provider or subscriber as a result of the communications.

6 Google is hereby ordered to disclose the above information to the government  
7 within 14 days of service of this warrant.  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28



**ATTACHMENT B**

**SUBJECT DEVICE to be Searched**

The SUBJECT DEVICE is further described as an electronic storage media, assembled in USA by DataLocker, serial number 04033416, currently in the custody of the Homeland Security Investigations at 1000 2<sup>nd</sup> Avenue, Suite 2300, Seattle, WA 98101. It is known as DataLocker (IronKey) H350 Encrypted External Hard Drive. The SUBJECT DEVICE is silver in color with black rubber trims. It is encrypted and passcode locked. SUBJECT DEVICE is accessible by USB port.

This warrant authorizes the forensic examination of the SUBJECT DEVICE for the additional purpose of identifying and seizing the electronically stored information described in Attachment C.

**ATTACHMENT C**

**Section I – Items to be searched:**

The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email, and any attachments to such emails;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, instant messages, and instant messenger contact information, calendar data, pictures, and files.

e. All records pertaining to communications between Google and any person regarding the account, including contacts with support services and records of actions taken.

**Section II - Items to be Seized**

1. All records on the SUBJECT DEVICE described in Attachment A that relate to violations of 18 U.S.C. § 2252(a)(2) (Receipt/Distribution of Child Pornography) and § 2252(a)(4)(B) (Possession of Child Pornography), including:

a. All messages, documents, and profile information, attachments, or other data that serves to identify any persons who use or access the account(s) specified, or who exercise in any way any dominion or control over the specified account(s);

- 1 b. Any address lists or buddy/contact lists associated with the specified account(s);
- 2 c. All images of child pornography, include "Image (13)" and " File
- 3 younowjoe\_jbs\_younow\_youtube\_cam0545.avi," and any messages, documents and
- 4 profile information, attachments, or other data that refer to child pornography or the
- 5 possession, receipt, or distribution of child pornography;
- 6 d. All subscriber records associated with the specified account(s), including name,
- 7 address, records of session times and durations, length of service (including start date)
- 8 and types of service utilized, telephone or instrument number or other subscriber number
- 9 or identity, (including any temporarily assigned network address, and means and source
- 10 of payment for such service) including any credit card or bank account number(s);
- 11 e. Any and all other log records, including IP address captures, associated with the
- 12 specified account(s); and
- 13 f. Any records of communications between Google Inc., and any person about issues
- 14 relating to the specified account(s), such as technical problems, billing inquiries, or
- 15 complaints from other users about the specified account(s). This is to include records of
- 16 contacts between the subscriber and the provider's support services, as well as records of
- 17 any actions taken by the provider or subscriber as a result of the communications.
- 18 g. Evidence of malware that would allow others to control any seized digital
- 19 device(s) such as viruses, Trojan horses, and other forms of malicious software, as well
- 20 as evidence of the presence or absence of security software designed to detect malware;
- 21 as well as evidence of the lack of such malware;
- 22 h. Evidence of the attachment to the digital device(s) of other storage devices or
- 23 similar containers for electronic evidence;
- 24 i. Evidence of counter-forensic programs (and associated data) that are designed to
- 25 eliminate data from a digital device;
- 26
- 27
- 28



1 j. Records of Internet Activity, including firewall logs, caches, browser history and  
2 cookies, "bookmarked" or "favorite" web pages, search terms the user entered into any  
3 Internet search engine, and records of user-typed web addresses.

4 2. This warrant authorizes a review of electronic storage media and electronically  
5 stored information seized or copied pursuant to this warrant in order to locate evidence,  
6 fruits, and instrumentalities described in this warrant. The review of this electronic data  
7 may be conducted by any government personnel assisting in the investigation, who may  
8 include, in addition to law enforcement officers and agents, attorneys for the government,  
9 attorney support staff, and technical experts. Pursuant to this warrant, the Homeland  
10 Security Investigations may deliver a complete copy of the seized or copied electronic  
11 data to the custody and control of attorneys for the government and their support staff for  
12 their independent review.